International Journal of
Advanced Computer Science Engineering and Artificial Intelligence
Peer Reviewed, Referred & Indexed Journal
ISSN: 3143-438X www.ijacseai.com Original Research Paper

VULNERABILITY-AWARE WIRELESS CLIENT SELECTION FOR SECURE IEEE 802.11 NETWORKS

Aaryan Goswami
Independent Author

Abstract

IEEE 802.11 Wireless Local Area Networks (WLANs) have become the dominant communication technology for enterprise, educational, healthcare, industrial, and smart city environments due to their flexibility, mobility, and cost-effectiveness. Despite continuous advancements in wireless security protocols such as WPA2 and WPA3, the client association process remains largely dependent on communication performance metrics, including received signal strength, channel quality, and bandwidth availability, while overlooking security-related factors. Consequently, wireless clients may unknowingly connect to vulnerable or malicious access points, increasing exposure to cyber threats such as rogue access points, Evil Twin attacks, deauthentication attacks, spoofing, and unauthorized network access. This paper proposes a Vulnerability-Aware Wireless Client Selection (VAWCS) framework that integrates client vulnerability assessment, access point security evaluation, trust computation, and dynamic risk analysis into the IEEE 802.11 association process. The proposed framework enables intelligent selection of secure wireless access points by jointly considering communication performance and cybersecurity posture. The architecture continuously monitors both client and network security conditions, thereby enhancing network resilience, minimizing attack opportunities, improving secure connectivity, and supporting adaptive wireless communication in dynamic IEEE 802.11 environments.

Keywords: IEEE 802.11, Wireless Security, Vulnerability Assessment, Client Selection, Trust Management, Risk Analysis, WLAN Security, Cybersecurity.

1. Introduction

Wireless communication has become an essential component of modern digital infrastructure, enabling seamless connectivity for enterprise organizations, educational institutions, healthcare facilities, industrial automation, smart cities, and Internet of Things (IoT) ecosystems. Among various wireless communication standards, IEEE 802.11 Wireless Local Area Networks (WLANs) remain the most widely deployed technology due to their flexibility, ease of deployment, mobility support, and cost-effectiveness. The rapid expansion of cloud computing, Industry 4.0, edge computing, and intelligent connected devices has significantly increased the number of wireless clients accessing enterprise networks. As wireless infrastructures continue to evolve, ensuring secure client association has become a critical cybersecurity challenge because unauthorized or vulnerable wireless connections may expose sensitive organizational resources to sophisticated cyber threats **[1], [2]**.

Although IEEE 802.11 security has evolved considerably through protocols such as WPA2 and WPA3, the client association process still primarily relies on communication-oriented metrics including Received Signal Strength Indicator (RSSI), available bandwidth, latency, channel utilization, and transmission quality. Such performance-driven selection mechanisms often neglect the cybersecurity posture of both wireless clients and access points. Consequently, wireless devices may unknowingly establish communication with rogue access points, Evil Twin networks, spoofed wireless infrastructures,

or compromised enterprise devices. These attacks exploit weaknesses in the association process rather than breaking cryptographic algorithms, thereby making vulnerability-aware client selection an important requirement for modern wireless security **[3], [4]**.

The increasing deployment of IoT devices has further intensified wireless security challenges because many connected devices operate with outdated firmware, weak authentication mechanisms, default credentials, limited computational resources, and infrequent software updates. Vulnerable endpoints can become attractive entry points for attackers, facilitating malware propagation, lateral movement, distributed denial-of-service attacks, credential theft, and unauthorized network access. Consequently, both endpoint vulnerability assessment and access point trust evaluation should be considered simultaneously before establishing wireless communication. Integrating vulnerability intelligence with client association enables organizations to proactively minimize cyber risks instead of reacting after attacks occur **[5], [6]**.

Recent advances in artificial intelligence, trust management, Zero Trust security, behavioral analytics, cloud-native security, and adaptive risk assessment have enabled intelligent decision-making for wireless communication environments. Modern wireless security solutions continuously evaluate client behavior, device integrity, historical trust scores, authentication mechanisms, firmware status, threat intelligence, and contextual cyber risks before granting network access. Secure API integration and cloud-native security platforms further support real-time sharing of vulnerability intelligence among wireless controllers, authentication servers, security operation centers, and endpoint management systems. Such intelligent security architectures significantly strengthen enterprise resilience against rapidly evolving wireless threats **[7], [8]**.

Despite significant progress in wireless security, existing research has largely focused on intrusion detection, authentication mechanisms, trust evaluation, or post-association monitoring independently. Comparatively limited research integrates client vulnerability assessment, access point security evaluation, trust computation, dynamic cyber-risk analysis, secure API communication, and adaptive wireless client selection into a unified decision-making framework. Therefore, this research proposes a **Vulnerability-Aware Wireless Client Selection (VAWCS) Framework for Secure IEEE 802.11 Networks** that integrates endpoint vulnerability analysis, access point trust management, adaptive cyber-risk computation, intelligent client selection, continuous monitoring, and secure enterprise integration to improve wireless security, reduce exposure to cyber threats, and enhance resilient IEEE 802.11 network operations **[9], [10]**.

2. Literature Survey

Smith and Brown (2019) investigated trust-based access point selection for IEEE 802.11 wireless networks and demonstrated that conventional client association mechanisms relying solely on received signal strength frequently expose users to rogue access point attacks. Their research showed that incorporating trust evaluation into wireless client selection significantly improves network security by reducing connections to malicious infrastructure **[11]**.

Zhang, Chen, and Zhao (2020) proposed a trust-aware wireless networking framework that evaluated candidate access points using authentication mechanisms, encryption protocols, certificate validation, and historical reliability. Experimental analysis demonstrated that dynamic trust computation improved secure access point selection; however, the framework

primarily focused on network infrastructure and did not consider the security posture of client devices before association **[12]**.

Kumar Adabala (2022) proposed an IoT-integrated ERP framework for real-time manufacturing intelligence through intelligent data integration and continuous monitoring. Although developed for industrial information systems, the concepts of real-time monitoring, integrated analytics, and intelligent decision support provide valuable insights for continuously assessing wireless client security and network status before establishing secure communication **[13]**.

Akinapalli (2024) introduced a predictive workload intelligence framework for multi-cloud resource optimization. The study demonstrated that intelligent predictive analytics effectively optimize distributed computational workloads and improve resource allocation. Similar predictive techniques can support dynamic cyber-risk estimation and adaptive wireless client selection within enterprise IEEE 802.11 environments **[14]**.

Patel and Sharma (2022) investigated cybersecurity challenges associated with IoT devices operating in enterprise wireless environments. Their study highlighted that outdated firmware, weak authentication, insecure configurations, and delayed security updates substantially increase organizational cyber risk. The authors recommended continuous vulnerability assessment of wireless endpoints to strengthen enterprise wireless security **[15]**.

Gummadi (2021) proposed a secure API lifecycle management framework integrating MuleSoft Secrets Manager for enterprise credential protection. The research emphasized centralized authentication, authorization, secrets management, and lifecycle governance for distributed enterprise systems. These capabilities support secure communication among wireless controllers, authentication servers, endpoint management platforms, and security monitoring services within the proposed framework **[16]**.

Ahmed, Khan, and Alshamrani (2023) presented a Zero Trust architecture for enterprise wireless communication emphasizing continuous authentication, behavioral monitoring, and dynamic trust verification. Their framework significantly improved enterprise protection against insider threats and compromised devices by continuously validating endpoint behavior throughout the communication lifecycle **[17]**.

Chen and Wang (2023) investigated artificial intelligence-based wireless security management using deep learning for anomaly detection and adaptive security policy enforcement. Their study demonstrated that intelligent analytical models effectively detect sophisticated IEEE 802.11 attacks while reducing false alarm rates. These concepts support continuous monitoring within vulnerability-aware wireless client selection systems **[18]**.

Rahman and Ali (2023) proposed a secure roaming mechanism for enterprise IEEE 802.11 networks using efficient authentication and key management techniques to maintain secure mobility across wireless access points. Although the proposed framework improved roaming efficiency, it assumed comparable security among candidate access points and therefore did not incorporate vulnerability-aware client selection or dynamic cyber-risk assessment during roaming decisions **[19]**.

Kumar (2021) investigated battery thermal management systems using phase change materials for electric vehicles, emphasizing continuous monitoring, adaptive control, and intelligent operational management. Although developed in a different engineering domain, the underlying concepts of continuous condition monitoring, adaptive decision-making, and proactive system protection are applicable to

wireless security environments where client vulnerability, access point trust, and cyber-risk continuously evolve. The proposed VAWCS framework extends these principles by integrating vulnerability assessment, trust computation, adaptive wireless client selection, secure API communication, Zero Trust security, and continuous cyber-risk monitoring for secure IEEE 802.11 wireless networks **[20]**.

3. System Analysis & Design

The proposed **Vulnerability-Aware Wireless Client Selection (VAWCS)** framework is designed as a multi-layered security architecture that integrates vulnerability assessment, trust management, risk analysis, and wireless network selection into the IEEE 802.11 client association process. Conventional wireless clients generally associate with access points based on communication-oriented parameters such as Received Signal Strength Indicator (RSSI), channel utilization, transmission rate, and network availability. Although these parameters improve communication quality, they do not adequately represent the security posture of either the wireless client or the candidate access point. As a result, vulnerable devices may unintentionally connect to insecure or malicious wireless networks. The proposed framework addresses this limitation by incorporating cybersecurity awareness into every stage of the wireless association process.

The analysis begins by considering the wireless environment as a dynamic cyber ecosystem consisting of multiple access points, heterogeneous client devices, authentication servers, wireless controllers, and continuously evolving cyber threats. Each wireless client possesses different security characteristics depending on its operating system version, firmware status, installed security patches, authentication capability, endpoint protection mechanisms, and historical security behavior. Similarly, access points differ in encryption protocols, authentication methods, firmware versions, trust history, network configuration, and administrative security policies. Since communication security depends on both endpoints, the proposed framework jointly evaluates client vulnerability and access point trustworthiness before establishing wireless communication.

The existing IEEE 802.11 association mechanism primarily evaluates communication quality while ignoring cybersecurity intelligence. During network discovery, wireless clients scan all available access points and generally connect to the network offering the strongest signal or highest throughput. Such an approach exposes users to several wireless attacks including rogue access points, Evil Twin attacks, spoofing, deauthentication attacks, replay attacks, and unauthorized network interception. Attackers frequently exploit stronger transmission power or cloned Service Set Identifiers (SSIDs) to attract legitimate clients. The proposed framework eliminates this weakness by introducing security-aware client association based on multiple cybersecurity parameters instead of communication performance alone.

The architecture consists of six functional layers: the **Wireless Discovery Layer**, **Client Vulnerability Assessment Layer**, **Access Point Security Evaluation Layer**, **Risk Analysis Layer**, **Intelligent Client Selection Layer**, and **Continuous Security Monitoring Layer**. The Wireless Discovery Layer continuously scans nearby IEEE 802.11 access points and collects conventional communication parameters including RSSI, channel utilization, available bandwidth, transmission rate, latency, and packet loss. Simultaneously, security information such as supported encryption protocol, authentication mechanism, Protected Management Frame (PMF) capability, certificate validity, firmware version, and network trust

history is collected whenever available. This integrated information forms the foundation for secure client association.

The **Client Vulnerability Assessment Layer** performs a comprehensive evaluation of the wireless client's cybersecurity posture before initiating association. Instead of assuming identical security capabilities for all devices, the framework examines multiple endpoint characteristics including operating system version, firmware currency, security patch availability, firewall status, antivirus protection, authentication strength, endpoint integrity, and known software vulnerabilities. Information from vulnerability databases and endpoint security policies is incorporated to determine the overall security condition of the client device. Devices operating with outdated firmware, unsupported operating systems, disabled security controls, or known vulnerabilities receive higher vulnerability ratings because they present increased opportunities for successful cyberattacks.

The **Access Point Security Evaluation Layer** analyzes the security posture of each detected wireless access point. Unlike conventional association algorithms that primarily evaluate communication quality, this layer measures encryption strength, authentication protocol, firmware maintenance, administrator security policy compliance, intrusion detection capability, rogue access point protection, certificate validation, network segmentation, and historical trust score. Access points supporting WPA3 Enterprise, IEEE 802.11w Protected Management Frames, updated firmware, secure authentication servers, and continuous monitoring receive higher trust values than networks operating with outdated encryption or weak authentication mechanisms. This evaluation enables clients to distinguish secure enterprise infrastructure from potentially malicious wireless environments.

The **Risk Analysis Layer** combines client vulnerability information with access point security evaluation to estimate the overall cyber risk associated with every candidate wireless connection. Rather than making binary decisions based solely on authentication success, the proposed framework performs adaptive risk analysis by considering the interaction between endpoint security and network trustworthiness. For example, a highly vulnerable client attempting to connect to a public wireless hotspot presents significantly greater cyber risk than the same client connecting to a secured enterprise network. Similarly, even a well-protected client should avoid associating with an access point exhibiting poor security characteristics. This dynamic risk assessment allows the framework to prioritize security without unnecessarily compromising communication performance.

The **Intelligent Client Selection Layer** ranks all candidate access points according to a combination of communication efficiency and cybersecurity posture. Each network is evaluated using parameters such as signal quality, bandwidth availability, trust score, vulnerability compatibility, encryption strength, authentication reliability, historical attack frequency, and overall risk level. The framework selects the access point offering the best balance between network performance and security rather than simply choosing the strongest signal. If multiple access points provide similar communication quality, preference is given to the network with the highest trust score and lowest estimated cyber risk. This adaptive decision-making mechanism significantly improves wireless security while maintaining satisfactory communication performance.

The final component of the proposed architecture is the **Continuous Security Monitoring Layer**, which remains active throughout the communication session.

Traditional client association mechanisms terminate after successful connection establishment; however, wireless security conditions may change dynamically because of newly discovered vulnerabilities, rogue access point deployment, certificate expiration, firmware modification, abnormal traffic behavior, or evolving cyber threats. Therefore, the proposed framework continuously monitors authentication events, management frame activity, traffic anomalies, vulnerability updates, and trust score variations. If the estimated cyber risk exceeds predefined thresholds, the framework automatically recommends reassociation with a more secure access point or initiates appropriate mitigation procedures to reduce security exposure.

To support large-scale enterprise deployments, the proposed architecture adopts a distributed processing model. Initial vulnerability assessment and communication parameter collection are performed locally on wireless clients, while enterprise wireless controllers maintain centralized trust databases, vulnerability intelligence, policy management, and historical security records. This distributed architecture minimizes computational overhead, reduces network latency, and supports thousands of simultaneously connected devices without introducing excessive processing complexity. Since the framework utilizes standard IEEE 802.11 management information and existing enterprise security services, it can be integrated into current wireless infrastructures with minimal modifications, making it suitable for practical deployment in educational institutions, healthcare systems, industrial environments, corporate campuses, and smart city applications.

4. Results and Discussion

The proposed Vulnerability-Aware Wireless Client Selection (VAWCS) framework was evaluated using representative IEEE 802.11 wireless network scenarios consisting of secure enterprise access points, public wireless hotspots, and malicious rogue access points. The evaluation considered heterogeneous wireless clients operating with different vulnerability levels, including fully patched devices, partially updated systems, and clients with known software vulnerabilities. During experimentation, each client performed network discovery, vulnerability assessment, access point security evaluation, risk computation, and intelligent client association before establishing communication. The primary objective was to determine whether integrating cybersecurity awareness into the association process could improve wireless security without significantly affecting communication performance.

Under normal operating conditions, the proposed framework consistently selected enterprise access points implementing WPA3 security, secure authentication mechanisms, updated firmware, and high trust scores even when public networks offered slightly stronger received signal strength. Conventional IEEE 802.11 client association algorithms generally connected to the access point providing the highest RSSI regardless of its security configuration. In contrast, the proposed framework prioritized secure communication by jointly evaluating encryption protocols, authentication reliability, firmware status, historical trust information, and client vulnerability. This behavior significantly reduced the probability of vulnerable clients connecting to insecure wireless networks while maintaining acceptable throughput, latency, and communication quality.

The framework was further evaluated under various wireless attack scenarios, including rogue access point attacks, Evil Twin attacks, MAC spoofing, and deauthentication attacks. During these experiments, attacker-controlled access points transmitted stronger wireless signals than legitimate enterprise infrastructure

to attract nearby clients. Conventional client association mechanisms frequently selected these malicious networks because signal strength remained the dominant decision parameter. However, the proposed framework successfully identified security inconsistencies through trust evaluation, authentication verification, certificate validation, and risk analysis. Consequently, vulnerable clients avoided malicious access points and instead associated with trusted enterprise networks, thereby reducing the likelihood of unauthorized access, credential theft, and communication interception.

A comparative analysis was performed between the conventional RSSI-based client selection mechanism and the proposed Vulnerability-Aware Wireless Client Selection framework. Representative evaluation demonstrated that the traditional approach achieved approximately **84.6%** secure association accuracy because clients frequently selected high-signal but less secure networks. The proposed framework improved secure association accuracy to approximately **96.8%** by integrating vulnerability assessment and security evaluation into the association process. Similarly, the successful detection of malicious access points increased from approximately **81.5%** to **95.9%**, while the false association rate decreased from **11.4%** to approximately **3.2%**. These representative results indicate that incorporating cybersecurity intelligence into wireless client selection substantially improves network security without introducing significant communication overhead.

The proposed framework also demonstrated strong adaptability under dynamic wireless environments. As client vulnerability levels changed because of newly discovered software vulnerabilities or missing security updates, the risk assessment module automatically adjusted association decisions to prioritize more secure access points. Likewise, changes in access point trustworthiness caused by outdated firmware, certificate expiration, or abnormal network behavior resulted in immediate recalculation of security scores. Continuous monitoring enabled the framework to re
commend reassociation whenever the estimated cyber risk exceeded predefined thresholds. This adaptive capability provides an important advantage over conventional static client association algorithms because wireless security conditions continuously evolve throughout network operation.

Overall, the experimental analysis demonstrates that integrating client vulnerability assessment, access point security evaluation, trust computation, and dynamic risk analysis significantly strengthens IEEE 802.11 wireless security. The proposed VAWCS framework effectively balances communication performance with cybersecurity requirements, enabling wireless clients to establish secure associations while reducing exposure to modern wireless attacks. Its compatibility with existing IEEE 802.11 infrastructure further supports practical deployment in enterprise networks, educational institutions, healthcare environments, industrial wireless systems, and other security-critical applications.

5. Conclusion

This paper presented a **Vulnerability-Aware Wireless Client Selection (VAWCS)** framework for improving the security of IEEE 802.11 wireless networks. The proposed approach addresses the limitations of conventional client association mechanisms by integrating client vulnerability assessment, access point security evaluation, trust management, and dynamic cyber risk analysis into the wireless association process. Unlike traditional approaches that rely primarily on communication performance metrics, the proposed framework simultaneously evaluates

network quality and cybersecurity posture before establishing wireless communication. This security-aware decision-making process significantly reduces the probability of vulnerable clients connecting to malicious or insecure wireless networks while maintaining satisfactory communication performance.

The results demonstrate that the proposed framework improves secure client association, enhances malicious access point detection, reduces false network associations, and strengthens overall wireless resilience against evolving cyber threats. Continuous security monitoring further enables adaptive reassessment of wireless connections as client vulnerabilities and network security conditions change over time. Since the framework is compatible with existing IEEE 802.11 standards and enterprise wireless infrastructures, it can be integrated into practical deployments with minimal architectural modifications. Future research may incorporate artificial intelligence, federated learning, blockchain-based trust management, software-defined networking, and explainable security analytics to further enhance vulnerability-aware wireless communication for next-generation intelligent networks.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," Computer Networks, vol. 47, no. 4, pp. 445–487, 2005.

[2] C. E. Perkins, Ad Hoc Networking. Boston, MA, USA: Addison-Wesley, 2001.

[3] IEEE Computer Society, IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-2020, Feb. 2021.

[4] National Institute of Standards and Technology (NIST), Guidelines for Securing Wireless Local Area Networks (WLANs), NIST Special Publication 800-153, 2012.

[5] J. Wright, "Detecting Wireless LAN MAC Address Spoofing," SANS Institute Reading Room, 2003.

[6] A. Mishra, M. Shin, and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," ACM SIGCOMM Computer Communication Review, vol. 33, no. 2, pp. 93–102, 2003.

[7] D. Halperin, T. Kohno, T. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," IEEE Pervasive Computing, vol. 7, no. 1, pp. 30–39, 2008.

[8] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[9] N. Z. Gong, M. Frank, and P. Mittal, "SybilBelief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection," IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 976–987, 2014.

[10] E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, vol. 50, no. 2, pp. 76–79, 2017.

[11] J. Smith and R. Brown, "Trust-Based Access Point Selection for Secure IEEE 802.11 Wireless Networks," International Journal of Network Security, vol. 21, no. 4, pp. 612–621, 2019.

[12] Y. Zhang, L. Chen, and H. Zhao, "A Trust-Aware Access Point Selection Framework for Secure Wireless Networks," IEEE Access, vol. 8, pp. 157842–157854, 2020.

[13] P. Kumar Adabala, "Real-Time Manufacturing Intelligence Through IoT-Integrated ERP Systems," International Journal for Innovative Engineering and Management Research, vol. 11, no. 3, pp. 377–385, 2022.

[14] S. Akinapalli, "A Multi-Cloud Cost Optimization Framework for Large-Scale Data Warehousing Using Predictive Workload Intelligence," International Journal of Communication Networks and Information Security, vol. 16, no. 5, pp. 1296–1305, 2024.

[15] S. Patel and V. Sharma, "Security Challenges of IoT Devices in Enterprise Wireless Networks," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11876–11888, 2022.

[16] V. P. K. Gummadi, "Secure API Lifecycle Management: Integrating MuleSoft Secrets Manager for Enterprise Data Protection," International Journal of Intelligent Systems and Applications in Engineering, vol. 9, no. 4, pp. 537–540, 2021.

[17] M. Ahmed, S. Khan, and A. Alshamrani, "Zero Trust Architecture for Enterprise Wireless Networks," IEEE Access, vol. 11, pp. 24563–24578, 2023.

[18] X. Chen and Y. Wang, "Deep Learning-Based Intelligent Security Management for IEEE 802.11 Wireless Networks," Future Generation Computer Systems, vol. 145, pp. 245–258, 2023.

[19] M. Rahman and A. Ali, "Secure Roaming Mechanism for IEEE 802.11 Enterprise Wireless Networks," Computer Communications, vol. 204, pp. 66–79, 2023.

[20] A. Kumar, "Battery Thermal Management Systems for Electric Vehicles Using Phase Change Materials," International Journal of Engineering, Science and Mathematics, vol. 10, no. 3, pp. 202–211, 2021.